# SOVEREIGNTY WITHOUT ENCLOSURE

SUM BUNNY

# SOVEREIGNTY WITHOUT ENCLOSURE

## Governing AI Infrastructure as a Buffer Commons

By Sum Bunny

2026

ARK HIVE PRESS

INTERNET ARCHIVE EDITION

OPEN THROTTLE

CC BY 4.0

# YOU ARE FREE

to share and adapt this material for any purpose, including commercially, provided appropriate credit is given.

https://creativecommons.org/licenses/by/4.0/

# CONTENTS


TITLE PAGE ..... 1

PLAIN-LANGUAGE SUMMARY ..... 2

TECHNICAL ABSTRACT ..... 3

I. WHO GETS TO SAY NO? ..... 4

II. THE MACHINE IS ALREADY PHYSICAL ..... 5

III. OPENNESS IS NOT YET A COMMONS ..... 7

IV. COMMONS WITHOUT EXIT CAN DOMINATE ..... 9

V. THE FOUR CONDITIONS OF THE BUFFER COMMONS ..... 11

VI. A 100-MEGAWATT TEST ..... 16

VII. POLITICAL GEOLOGY AND THE LIMITS OF LOCALISM ..... 19

VIII. THE HARD OBJECTIONS ..... 20

IX. SOVEREIGNTY AS A MAINTAINED CAPABILITY ..... 23

ENDNOTES ..... 24

AI ASSISTANCE DISCLOSURE ..... 25

CANON NOTE ..... 26


Essay page numbers are retained from the author’s publication master.
Cover, edition matter, and Transmission are unnumbered supplementary pages.

# SOVEREIGNTY WITHOUT ENCLOSURE

*Governing AI Infrastructure as a Buffer Commons*

**SUM BUNNY**

2026

**No expansion without headroom.**

**No consent without the power to refuse.**

**No innovation without funded repair.**

## PLAIN-LANGUAGE SUMMARY

Imagine that a company wants to build a very large AI data center near a city. It may bring jobs and useful computing power. It may also use large amounts of electricity and water. It may require new public infrastructure.

The company can threaten to build elsewhere. It can afford to leave. Most nearby residents cannot. If the project fails, they may still be left with higher bills, public debts, strained services, or abandoned infrastructure. That difference in who can walk away leads to the essay's central question: **Who really has the power to say no?** Technological sovereignty usually means owning or controlling important technology. But ownership alone does not make people free. A government can own servers while workers and residents cannot influence how they are built, used, or repaired.

This essay calls its alternative the **Buffer Commons**. It means protecting the spare capacity and recovery resources around a powerful technology because the public depends on them. A project cannot consume everything that keeps the larger system safe. People who bear its risks need enforceable rights, not invitations to comment. The proposal has four parts.

**Leave enough spare capacity.** The project must preserve enough electricity, water, emergency services, and public resources for ordinary needs and unexpected failures.

**Give affected people a real say.** Affected groups must be able to change decisions before the project's terms are settled. A hearing that cannot change the outcome is not public control.

**Make refusal possible.** Refusal is not meaningful if it means losing income, housing, healthcare, essential services, or ordinary public support. Rights must include the practical means to survive using them.

**Prepare and pay for repair.** Before a project begins, money, plans, and legal authority must exist for shutdown, cleanup, worker transition, abandoned infrastructure, and foreseeable damage. Promises after failure are not recovery capacity.

$D \leq R$ means that new demand must not use more than the surrounding system can safely absorb and recover from. It is not one magic score. Electricity, water, worker safety, and public cost must each be judged on their own terms. A benefit in one area cannot erase serious harm in another.

A hypothetical 100-megawatt data center shows how this could work. The project must disclose what it uses, who carries its risks, and who pays if it expands, closes, or fails. Public bodies would monitor the agreement, people could appeal decisions, and repair funds would exist before they are needed. That is sovereignty without enclosure.

## TECHNICAL ABSTRACT

Technological sovereignty is commonly understood as the ability of a nation, corporation, or community to control the technologies on which it depends. That definition is incomplete. A state can possess domestic data centers, sovereign cloud infrastructure, and open-source software while residents remain unable to influence deployment, workers remain unable to refuse dangerous conditions, and public systems absorb the costs of private expansion. Openness can coexist with domination; local control can coexist with exclusion; national sovereignty can become another form of enclosure.

This essay proposes the Buffer Commons as a different model. A technological system is democratically sovereign only when those who bear its risks possess four enforceable capabilities: protected physical headroom, accountable voice in the rules, material power to refuse participation, and funded capacity to recover from failure. Applied to artificial-intelligence infrastructure, the model converts the Opal Architecture's general constraint—development must not consume the capacity required to survive development—into a polycentric institutional protocol. Its central rule, $D \leq R$, is not treated as a universal numerical score but as a constitutional instruction implemented through separate domain-specific limits on grid load, water use, fiscal exposure, labor harm, and recovery capacity. A worked example involving a hypothetical 100-megawatt data center demonstrates how lifecycle boundary declarations, public telemetry, periodic category audits, proportional obligations, cost-recovery agreements, resilience bonds, representation, appeal, and unconditional refusal power could operate together. The result is neither unrestricted acceleration nor centralized prohibition, but sovereignty understood as a maintained public capability: the power to set limits, decline unacceptable terms, revise the categories through which harm is seen, and remain able to repair what technological expansion places at risk.

## I. WHO GETS TO SAY NO?

Imagine that a company proposes a 100-megawatt artificial-intelligence data center outside a growing American city.

It does not arrive as a robot. It arrives as a packet of contracts: a land purchase, an interconnection request, a water agreement, a tax proposal, a construction schedule, a projected payroll, and a promise that delay will send the investment somewhere else. The company has engineers, attorneys, consultants, lobbyists, and several possible jurisdictions. The utility sees a major new customer. Public officials see construction, prestige, and revenue. National policymakers see strategic infrastructure in a global competition over artificial intelligence.

The people who already live there encounter the project differently. They may see employment and investment. They may also see new transmission equipment, water consumption, diesel backup generation, altered land use, ratepayer exposure, and a facility whose operational logic they cannot inspect. The developer can threaten to leave. Most residents cannot. The company can hire experts to describe the project. The public may have to learn the system quickly, after its basic terms have already been negotiated.

This is normally presented as a dispute over growth: How much development can a region accommodate? But underneath it lies a more important question.

**Who actually possesses the power to say no?**

If a company can refuse a jurisdiction but a worker cannot refuse a dangerous job, the bargaining relationship is not symmetrical. If a locality cannot afford to reject a tax base, its approval is not wholly voluntary. If residents can speak at a hearing but cannot alter the operating agreement, their participation may be expressive without being governing. If the public will inherit abandoned infrastructure or higher rates after a failed project, consent at the beginning does not settle responsibility at the end.

This is the concealed problem inside many discussions of technological sovereignty. Sovereignty is usually assigned to the actor that owns the asset, controls the code, regulates the territory, or possesses the supply chain. But ownership and control do not by themselves establish freedom. They may merely identify the enclosure and its manager.

Artificial intelligence makes this problem unusually visible because the technology combines two apparently opposite qualities. Its outputs seem immaterial: words, images, classifications, predictions, software, and synthetic media. Its production is intensely physical: chips, land, cables, substations,

cooling systems, water, backup generators, mines, factories, warehouses, and human labor. The intelligence may be distributed through a network, but its burdens land somewhere.

The United States Department of Energy reported that data centers consumed approximately 4.4 percent of US electricity in 2023 and projected that their share could rise to roughly 6.7 to 12 percent by 2028.[1] The range is uncertain, but the institutional question does not depend on the highest estimate proving correct. When a single class of infrastructure can materially reshape regional electricity demand, technological policy can no longer treat compute as an abstract quantity floating above the grid.

Nor can it assume that any public concern about limits is hostility to invention. A society that preserves no headroom for heat waves, drought, maintenance, price shocks, transmission failures, or human emergencies is not maximizing intelligence. It is spending its ability to recover.

The alternative proposed here is a **Buffer Commons**: a system in which the people who produce, depend upon, and bear the costs of technological infrastructure possess enforceable authority over the reserves that keep the larger system inhabitable. The Buffer Commons does not require every server to be collectively owned or every technical decision to be decided by referendum. It requires something more precise. Before a high-impact system expands, four conditions must be secured:

1. **Protected buffer:** the system must preserve measurable headroom in each critical physical domain.
2. **Accountable voice:** affected people must possess real decision rights, not merely opportunities to comment.
3. **Material refusal:** individuals and communities must be able to reject unacceptable terms without being threatened with destitution or institutional abandonment.
4. **Funded repair:** the resources and authority required for recovery, maintenance, closure, and redress must exist before harm occurs.

No expansion without headroom. No consent without the power to refuse. No innovation without funded repair.

That is technological sovereignty without enclosure.

## II. THE MACHINE IS ALREADY PHYSICAL

The mythology of artificial intelligence encourages a category mistake. We speak of models as though they reside in a placeless realm called “the cloud.” We measure capability in parameters, operations, benchmark scores, and tokens. We describe deployment as a software event even when it reorganizes a workplace, changes access to housing or credit, or increases the demand placed on an electrical system.

The Opal Architecture begins from the opposite direction. It treats technological capacity as inseparable from the material and institutional buffers that capacity consumes. Its recurring diagnosis is **Buffer Mining**: a system appears productive because it converts hidden reserves into visible output. Maintenance is deferred, spare capacity is eliminated, public infrastructure absorbs private demand, workers absorb volatility, and ecosystems absorb waste. The balance sheet records the new product but not the diminished ability of everything around it to withstand shock. That omission is **Ledger Myopia**.

Markets can coordinate many immediate exchanges remarkably well. They can price land, electricity contracts, cooling equipment, construction labor, and access to processors. But a market price does not automatically reveal who will pay for an unused substation if a planned facility is abandoned, what reserve a community will need during a drought, how much institutional knowledge disappears after outsourced workers leave, or how the bargaining power of residents changes when a locality becomes dependent on one taxpayer. Some of these costs can be priced. Others require rights, prohibitions, public judgment, and institutions capable of looking beyond a transaction.

Recent US electricity regulation demonstrates that even conventional institutions are beginning to confront one part of this problem. In June 2026, the Federal Energy Regulatory Commission issued six show-cause orders directing regional grid operators to justify or reform the tariffs governing connections by data centers and other large loads. Commissioner David Rosner described Cost Recovery Agreements intended to ensure that large customers pay their fair share of infrastructure built to serve them, including when anticipated demand fails to materialize and would otherwise leave residential customers with the cost.[2]

That is not yet a Buffer Commons. It is, however, an important recognition: infrastructure risk should follow the project that creates it rather than disappear into the public system.

The Opal Architecture expresses its broad constraint as:

$$\mathrm{D} \leq \mathrm{R}$$

Development or demand, $\mathrm{D}$, must not exceed the system's ability to absorb disturbance and recover, $\mathrm{R}$.

Taken literally as a universal equation, this fails. Electrical load, groundwater depletion, emergency response, wage deterioration, biodiversity, fiscal dependency, and political legitimacy do not share a common unit. Any attempt to combine them into one score would conceal moral judgments inside mathematical weights. The result would be the very technocracy the framework is intended to prevent.

The equation is therefore better understood as a **constitutional instruction**, not a master measurement. Operationally, it becomes a family of separate constraints:

$$\mathrm{L_i} + \mathrm{B_i} \leq \mathrm{C_i}$$

For every critical domain $i$:

- $L_i$ is the load imposed by the proposed system;
- $B_i$ is the protected reserve required for uncertainty, maintenance, shock, and recovery;
- $C_i$ is the verified sustainable capacity of that domain.

Electricity must be evaluated as electricity. Water must be evaluated as water. Emergency capacity must be evaluated as emergency capacity. Fiscal exposure must be evaluated under plausible failure and abandonment scenarios. Labor conditions and social harms require quantitative evidence where appropriate, but also testimony, history, law, and rights that cannot be traded away because an aggregate score remains positive.

Failure in one critical domain can stop or reshape a project. An abundance of tax revenue does not cancel an exhausted aquifer. A community-benefit payment does not purchase permission to violate civil rights. Additional generation does not erase a transmission constraint. A high model-safety score does not pay for a stranded substation.

This is the **Categorical Boundary of Mathematics** within the Opal Architecture. Measurement is essential, but jurisdiction matters. Numbers may reveal whether an engineering buffer is shrinking. They must not be used to calculate the moral worth of a person, convert dignity into a score, or allow one kind of benefit to erase an incommensurable harm.

The practical implication is straightforward: there is no single “safe” number for technological development. There is a set of protected conditions that expansion is not permitted to consume.

## III. OPENNESS IS NOT YET A COMMONS

The language of the commons is attractive because it seems to offer an escape from both corporate monopoly and centralized government control. If proprietary technology encloses knowledge, make the code open. If a company monopolizes infrastructure, turn it into a public utility. If national agencies govern from a distance, move authority to workers and communities.

Each move may be valuable. None automatically creates a durable commons.

Elinor Ostrom’s work is often summarized as proof that communities can govern shared resources without privatization or centralized command. The more demanding lesson is that successful commons are institutions, not moods. They establish boundaries around resources and membership. Rules fit local conditions. People affected by operational rules can participate in changing them. Monitors are accountable. Sanctions are proportionate. Conflict-resolution mechanisms are accessible. External

authorities recognize the right of participants to organize. Larger systems are organized through nested layers of authority.[3]

Open access alone may produce no such arrangement. A software repository can be open while a handful of maintainers perform exhausting unpaid labor. Model weights can be downloadable while the training data remains undisclosed, compute remains prohibitively expensive, and downstream users possess no recourse. A public data set can be technically accessible while the people represented in it have no collective authority over its use. A municipally owned facility can still be captured by contractors, local elites, or exclusionary majorities.

Artificial intelligence also contains several different kinds of resource. Energy and high-end compute are rivalrous: one user's consumption can reduce what remains available to another at a particular time and place. Software and model weights can be copied, but their security, documentation, hosting, evaluation, and maintenance require scarce labor and infrastructure. Data may be reproducible while still carrying privacy, provenance, cultural, and collective-rights obligations. Evaluation knowledge may need broad circulation, while some dangerous details require protected disclosure.

These resources cannot be governed by one romantic picture of "the community." They require different rules, boundaries, institutions, and scales.

This is increasingly recognized in the literature. A 2026 preprint proposes "commons-governed artificial intelligence" as an institutional family spanning data, compute, models, knowledge and evaluation, and energy. It uses Ostrom's principles to classify data cooperatives, public compute, open-model collaborations, and other arrangements, while acknowledging dangers including openwashing, free-riding, compute concentration, and conflicts between scale and sustainability.[4] European governments have also begun creating institutional mechanisms for digital commons and technological sovereignty, including the Digital Commons European Digital Infrastructure Consortium, whose stated purpose includes developing open, interoperable, reusable infrastructure across borders.[5]

These developments matter because they eliminate an easy novelty claim. "AI should be a commons" is no longer a sufficient thesis. Nor should the commons be presented as an untouched space between evil markets and evil states. Markets, public agencies, courts, standards bodies, cooperatives, utilities, unions, and local governments can all perform necessary functions within a polycentric order.

The unresolved problem lies elsewhere.

A commons can be collectively governed and still dominate individual members. A town can democratically accept an arrangement that exposes a minority neighborhood to concentrated harm. Workers can collectively control an enterprise yet remain trapped if leaving means losing housing, healthcare, income, or legal status. A nation can achieve technological independence by intensifying

extraction somewhere else. A local veto can protect a wealthy enclave while transferring infrastructure to a poorer jurisdiction.

Collective voice does not guarantee individual freedom. Openness does not guarantee meaningful access. National control does not guarantee democratic control. Localism does not guarantee justice.

The missing condition is the material power to refuse.

## IV. COMMONS WITHOUT EXIT CAN DOMINATE

Two traditions clarify the missing condition, but they should not be converted into imaginary endorsements. Before turning to them, the institutional problem can be stated directly: rules must be evaluated not only by their stated purpose but by the distribution of power they produce.

Who decides which questions are considered reasonable, which risks receive institutional attention, and who is allowed to count as an expert? A safety requirement that only the largest corporations can afford may reduce one risk while creating a durable monopoly. A participatory process designed by the developer may manufacture legitimacy without transferring authority. This does not prove that every licensing proposal is corporate capture or every technical expert is compromised. It establishes a discipline of inquiry: examine who can set the agenda, withhold information, finance compliance, survive delay, and exit the jurisdiction.

bell hooks' work insists that domination must be examined from the position of people made peripheral by established institutions.[6] Applied to artificial intelligence, this changes both the evidence and the time horizon. The relevant system includes not only frontier researchers and hypothetical future victims but also data workers, warehouse and construction workers, communities near extraction and infrastructure, people subjected to automated decisions, and populations asked to surrender privacy or autonomy as the price of participation.

This does not require choosing present harm over future catastrophe. That opposition is another false binary. A governance system that ignores present exploitation will lack legitimacy and information. A system that ignores catastrophic and intergenerational danger will mistake immediacy for justice. Temporal justice asks the same questions across time: Who receives the benefit? Who bears the risk? Who can alter the decision? Who remains able to recover?

Karl Widerquist supplies the most direct account of refusal. His theory of freedom as independence argues that formal choice is insufficient when people lack secure access to the resources needed to survive. A person offered several masters but no viable ability to reject all of them does not possess

meaningful freedom.[7] Unconditional Basic Income is valuable in this account not merely because it relieves poverty, but because it changes bargaining power. It gives people the material ability to say no.

That principle transforms the commons.

Participation cannot be called voluntary when declining it means hunger, homelessness, loss of healthcare, deportation, or the abandonment of an entire locality. Consultation cannot establish consent when one side controls the technical evidence and the other side cannot afford independent counsel. A community cannot negotiate as an equal when public services have been deliberately starved and a private project is presented as the only rescue available.

This does not mean every technological decision must wait for a complete national UBI. It means governance must recognize **refusal capacity** as an institutional requirement rather than treating desperation as consent.

At the level of a project, refusal capacity can include:

- independent technical assistance controlled by affected communities;
- non-retaliation and whistleblower protection for workers;
- transition income for workers displaced by closure or automation;
- unconditional community dividends from the use of scarce public resources;
- public alternatives when an AI-mediated service would otherwise be compulsory;
- relocation, remediation, or buyout options where harms cannot be sufficiently reduced;
- legal representation and accessible appeal;
- protection against utility shutoff, eviction, or loss of essential services during disputes.

These measures are partial. They do not equal a universal, sufficient, unconditional income. A larger theory of technological freedom may still require UBI funded through a broad and durable fiscal base, potentially including resource rents, land value, capital income, pollution, and some forms of highly concentrated automated production. A compute fee alone should not be advertised as capable of funding the entire obligation without evidence. Its revenue may be volatile, geographically uneven, and vulnerable to avoidance.

Nor may basic income be conditioned on “civic stewardship.” If a person must perform approved maintenance, auditing, environmental repair, or community service to receive it, the income is no longer unconditional. Civic and maintenance work can be supported, honored, and paid. It cannot be smuggled back in as the price of survival.

This distinction is decisive. The purpose of independence is not to compel better work. It is to make cooperation genuinely voluntary. People freed from coercive dependence may choose care, repair,

invention, leisure, family, art, political participation, paid employment, or forms of work that institutions do not know how to count. A liberated commons does not assign their moral worth.

It protects their standing to refuse.

## V. THE FOUR CONDITIONS OF THE BUFFER COMMONS

The Buffer Commons combines physical constraint, collective governance, individual independence, and recovery finance. None can substitute for the others.

### 1. Protected Buffer

Every high-impact project begins by identifying the critical systems it will load. For a data center, these may include electricity generation and transmission, local distribution equipment, water, land, air quality, emergency response, transportation, housing, municipal finance, construction labor, and cybersecurity.

Public health is a protected domain wherever a project could plausibly affect noise, sleep, air quality, heat, drinking water, occupational conditions, or access to emergency services.[8] Those burdens must be evaluated at the spatial and temporal scale at which people experience them. A regional average, global offset, or benefit delivered elsewhere cannot erase a concentrated local burden.

Each domain receives its own baseline, uncertainty range, safety reserve, monitoring method, and intervention rule. These are not chosen entirely by the developer. They are established through publicly reviewable standards and adjusted to local conditions by institutions representing the people exposed to the result.

A baseline is not automatically a legitimate floor. Existing deprivation, pollution, deferred maintenance, or unreliable service cannot be relabeled as sustainable capacity merely because it is normal. Where a host system is already below a legally or democratically protected minimum, new load must wait, shrink, or supply additional restorative capacity before it can claim any remaining headroom.

The Opal Architecture calls the continuing observation of these reserves **Net Buffer Telemetry**. The term “telemetry” should not be allowed to imply that every relevant fact arrives from an automated sensor. Grid frequency, load, transformer temperature, water withdrawal, emissions, and equipment state can often be measured instrumentally. Wage deterioration, discriminatory impact, fear, cultural loss, institutional dependency, and community trust require different forms of evidence. Administrative records, surveys, interviews, complaints, public hearings, worker reports, and independent research belong in the system too.

The distinction protects both science and democracy. A water meter should not be overruled by a public-relations campaign. A worker's experience should not be dismissed because it is not a voltage.

Telemetry is also vulnerable to manipulation. Sensors fail. Baselines are chosen strategically. Companies optimize reported metrics. Agencies lose expertise. Uncertainty is suppressed to make a project appear inevitable. For that reason, credible Net Buffer Telemetry requires redundant sources, published methodologies, audit access, conflict-of-interest rules, uncertainty bands, data retention, and procedures through which affected people can challenge the measurement itself.

A monitoring system also needs protected human reporting channels. Workers and contractors must be able to report manipulated telemetry, suppressed uncertainty, or unsafe operating practices through confidential channels administered independently of the operator. Anti-retaliation remedies, legal support, and continuity of income and benefits during a protected disclosure are part of the epistemic infrastructure, not optional employment benefits.

Even accurate telemetry inherits the blind spots of the categories it monitors. A dashboard can show every chosen variable perfectly while excluding a harm that never became a field. The institution therefore needs a periodic category audit: What consequences failed to appear? Whose experience cannot be expressed in the accepted schema? Has scale replaced thick local knowledge with a thin proxy? Which once-useful category has become entrenched? This second-order review must be able to add or retire measures, revise baselines and triggers, and commission new forms of evidence without weakening the rights floor.

Approaching a boundary should not trigger an improvised emergency. The operating charter must define staged responses in advance. A normal range permits operation and ordinary inspection. A stressed range can pause expansion, increase reporting, activate conservation measures, or call contracted demand response. A critical range can require controlled curtailment under technically feasible rules, with exceptions for functions whose abrupt interruption would create greater danger. A failure condition releases recovery resources and transfers defined authority to emergency institutions.

Each domain also needs a failure-time map. The operating charter should state how quickly a loss of grid power, cooling, water, network service, fuel, or critical labor could produce unsafe conditions; how facility load ramps or trips; how long backup systems can sustain essential functions; how much notice an intervention requires; and which actor can act within the available window. The map should identify the shortest credible Time-to-Danger among exposed populations rather than report only an average condition, and it should test compound, multi-day failures. A buffer is not only a quantity. It is also time in which recognition, deliberation, and escape remain possible.

The assessment horizon for each domain must extend through its plausible recovery cycle. A resource that replenishes over centuries cannot be represented as a temporary draw within a short operating covenant. Where restoration cannot be demonstrated within the relevant ecological and institutional horizon, the burden must be treated as depletion rather than recoverable use.

“Fail slow” is not a promise that every failure can be made gentle. It is a design obligation to create time for human recognition, intervention, and escape wherever time can be created.

## 2. Accountable Voice

The phrase “affected community” cannot remain ceremonial. The institution must identify who is affected, in what way, and with what authority.

For a large data center, the relevant public may include host-community residents, ratepayers across a utility territory, utility and facility workers, Tribal nations, farmers and other water users, nearby jurisdictions, emergency personnel, future ratepayers, and populations disproportionately exposed to pollution or displacement. Ecological and intergenerational interests require representation through institutions with duties that extend beyond the current election or contract. People affected by the AI systems running inside the facility may be geographically distant and governed under a separate application-level regime.

Tribal nations are not merely another stakeholder category. Where sovereignty, treaty rights, territorial rights, or statutory consultation duties apply, those authorities and obligations must be honored on their own terms; a general community board cannot absorb or waive them.

These groups have overlapping but nonidentical interests. Facility workers may favor expansion that strains the grid. Nearby residents may oppose infrastructure whose regional benefits are substantial. A host locality may accept a project that transfers costs to ratepayers elsewhere. A national government may invoke security to override local knowledge. No single group can stand in for everyone.

Authority must therefore be polycentric and nested:

- national and international institutions establish rights floors, trade rules, catastrophic-risk duties, and restrictions on harms no locality may authorize;
- regional grid bodies and utilities govern interconnection, reliability, transmission cost, and curtailment;
- states govern utility rates, water, environmental review, taxation, and corporate obligations;
- local and Tribal governments govern land use, local services, and host-community conditions within their lawful authority;
- worker organizations govern workplace representation, safety, and refusal rights;

- community oversight bodies monitor performance, allocate defined benefits, initiate complaints, and review expansion.

Local power is necessary but not innocent. A direct local veto can become a mechanism by which affluent communities divert unwanted infrastructure to places with less political capacity. A town majority can sacrifice a neighborhood. A community board can be captured by contractors or prominent property owners. The answer is not to return all power to a distant center. It is to establish representation rules, transparency, conflict-of-interest prohibitions, minority protections, regional coordination, affordable appeal, and a non-waivable rights floor.

Voice is real only when it can alter an outcome. A hearing after the interconnection agreement is effectively settled is not governance. A comment period without access to the underlying assumptions is not governance. A community-benefit agreement negotiated by people selected by the developer is not governance.

The relevant test is simple: **What decision can the public body actually change, and what happens when it says no?**

## 3. Material Refusal

Collective voice and individual refusal solve different problems.

Voice gives people standing within a decision. Refusal protects them when the collective decision is unacceptable, when institutions fail, or when dependence makes participation coerced. A worker needs the right to report a dangerous practice without losing the means to live. A resident facing a severe localized burden needs more than the knowledge that the project won a regional vote. A person subjected to a consequential automated system may need a human alternative, not merely representation on a general advisory board.

Refusal rights must therefore be backed by resources. A formal right that predictably produces destitution is a weak right. The exact mechanism will vary by scale, but the institutional purpose remains constant: reduce the penalty for saying no.

For workers, this may include income continuity, portable benefits, union protection, whistleblower remedies, and compensation during safety shutdowns. For residents, it may include unconditional dividends, remediation, legal support, property protections, or relocation chosen by the resident rather than imposed by the project. For users of public services, it may include a non-digital or non-AI pathway where automated participation would violate autonomy, accessibility, due process, or privacy.

The word “unconditional” matters. A community dividend cannot become payment for silence. Worker transition support cannot require surrendering a legal claim. Technical assistance cannot be withdrawn

because the community opposes the project. The resources that make refusal possible must not be controlled by the party whose terms are being refused.

Unconditional refusal does not mean that one person's objection resolves every collective decision. It means that exercising a protected refusal right is not contingent on wealth, payment, service, or developer-defined conduct. Individuals control their own labor and participation; collective infrastructure decisions follow legitimate public procedures; sovereign nations and other rights-holders retain their distinct authority; and no majority may waive the rights floor or the Shielded Core.

Nor may a locality be billed for declining a project or lose ordinary public support because it said no. Fiscal equalization should reduce desperation before bargaining begins and must be financed independently of any particular refusal. It cannot become a refusal tariff that turns consent into a luxury good.

## 4. Funded Repair

Promises made after failure are not recovery capacity.

Before operation begins, the project must capitalize the obligations it could otherwise externalize. These may include grid upgrades, water infrastructure, emergency services, environmental remediation, equipment removal, site restoration, worker transition, long-term monitoring, and the maintenance of resilience assets created as part of the agreement.

The Opal Architecture calls this precondition the **Genesis Constraint**: a system should not begin generating high-impact output until the means of containing and recovering from its foreseeable failure exist. In infrastructure governance, that means money, authority, plans, and physical capacity—not a corporate assurance that the company intends to behave responsibly.

Financial assurance can take several forms: funded trusts, surety bonds, letters of credit, insurance, cost-recovery agreements, and other instruments designed to keep resources available for closure and repair. Environmental regulation already uses such mechanisms to secure closure and post-closure obligations.[9] Their protection against insolvency varies. The exact instrument therefore matters: it must be adequately sized, independently verified, replenished as conditions change, legally reachable when triggers occur, and protected from the operator's ordinary creditors to the greatest extent the governing law permits.

Financial assurance cannot convert irreparable harm into purchasable permission. If a credible failure would violate a non-waivable right, cross a protected minimum, or cause damage that cannot be contained and repaired, the Genesis Constraint requires redesign or denial—not a larger bond.

Community resilience investments should also satisfy additionality and ownership tests. A company should not receive credit for infrastructure it was already required to build for its own operation. A "community microgrid" that primarily serves the data center is not a public resilience asset. A cooling reservoir inaccessible during emergency conditions is not public water security. Assets created for the community should be selected through legitimate public processes, maintained through dedicated funding, and owned or controlled by institutions that survive the developer's departure.

These protected recovery assets form the **Shielded Core**. Expansion may fluctuate around them. The Shielded Core is not mined for quarterly performance, pledged as collateral for unrelated risk, or quietly reclassified as excess capacity. Its purpose is to remain available when ordinary optimization has failed.

## VI. A 100-MEGAWATT TEST

Consider again the hypothetical 100-megawatt facility. The scale is adapted from Amelia Michael's GovAI technical report comparing the total cost of building and operating a hypothetical 100-MW data center in the United States and the United Arab Emirates.[10] Here it serves a different purpose: an institutional stress test. The report's total-cost-of-ownership model is useful within its stated boundary, but it is not treated as a complete account of social cost, public risk, or consent.

Under ordinary development logic, separate institutions may review pieces of the proposal: land use, electricity, water, environmental effects, taxes, and construction. The Buffer Commons does not erase these jurisdictions. It connects them through a lifecycle covenant so that no institution assumes another has protected the public system.

### Before Approval

The developer submits a public infrastructure-impact statement using standardized definitions. It must state whether "100 megawatts" means information-technology load, total facility load, maximum contracted demand, or peak grid withdrawal, and disclose the efficiency and utilization assumptions connecting those figures. It includes expected and peak electricity demand, proposed ramp rates, backup generation, water consumption under ordinary and extreme weather, construction demands, expected employment, tax treatment, expansion scenarios, abandonment scenarios, and any operational flexibility the company is prepared to guarantee.

Because every metric has a fence line, the statement also declares its lifecycle boundary. It identifies direct facility burdens, enabling grid and water infrastructure, upstream generation and fuel, construction materials, equipment replacement and electronic waste, off-site pollution, and

decommissioning. A cost does not disappear merely because the project moves it beyond the property line or national border.

The statement includes the failure-time map required by the operating charter and distinguishes nameplate capacity from credible operating behavior. It tests ordinary conditions, extreme weather, delayed interconnection, partial buildout, sudden changes in demand, ownership change, and abandonment rather than relying on a single annual average.

The project pays a nonrefundable assessment fee into an independent public fund. Affected communities use that fund to retain technical and legal expertise of their own choosing. The experts owe duties to the public body, not to the developer.

Each competent authority defines its protected buffer. The grid authority considers generation adequacy, transmission, distribution, reliability, queue effects, and the possibility that promised demand arrives late or not at all. Water authorities consider drought and cumulative withdrawal rather than annual averages alone. Municipal analysts test revenue claims against abatements, service costs, infrastructure depreciation, and failure scenarios. Labor and housing assessments examine not merely the number of jobs but their duration, quality, recruitment pattern, and possible displacement effects.

The project cannot cancel a failure in one domain by overperforming in another. It must redesign, reduce load, fund new capacity, accept enforceable operating limits, or be denied.

## The Two-Axis Risk Rule

Physical infrastructure and artificial-intelligence capability must not be collapsed into one regulatory tier.

The facility's physical obligations scale with electricity, water, land, emissions, and infrastructure exposure. The AI system's safety obligations scale with capability, use, autonomy, access, and consequence. A small model embedded in emergency dispatch or weapons targeting can create grave functional risk while consuming little electricity. A large facility performing comparatively ordinary scientific or commercial computation can create substantial physical demands without running the most dangerous model.

Colocation, cloud tenancy, and rapidly changing workloads complicate the functional axis. The facility operator may not know every downstream use, and some information may legitimately require protection. Even so, the responsible developer or tenant must provide enough verified information to the competent functional regulator to classify risk. Public reporting can be aggregated or securely redacted, but commercial secrecy cannot become a functional-risk exemption.

Openness is relevant to auditability, competition, research, and public access. It is not a presumption of harmlessness. Proprietary systems are not automatically dangerous, and open systems are not automatically safe.

The result is proportional regulation without a flat innovation moat: small developers and public-interest researchers receive accessible compliance pathways and shared audit resources, while obligations rise with demonstrated physical and functional risk. The European Union's AI Act already demonstrates the general principle that regulation can vary according to risk, even though the Buffer Commons would use different categories and would add physical infrastructure and refusal power to the analysis.[11]

## The Operating Covenant

Before connection, the developer signs enforceable cost-recovery and operating agreements. Project-caused grid upgrades are not shifted to residential customers merely because ordinary rate design makes the transfer obscure. The agreement specifies what happens if construction is delayed, demand is lower than promised, the facility expands, or the company abandons the site.

Where technically feasible, the facility contracts for staged demand response. The contract identifies which loads can be reduced, how much notice is required, which conditions trigger action, who possesses override authority, and what safety functions cannot be interrupted. "Automated load shedding" is not treated as magic. It is an engineered and legally accountable capability tested before it is needed.

A resilience bond capitalizes closure, restoration, worker transition, and the community's selected infrastructure protections. Funds are recalculated at scheduled intervals and after material expansion. The community's portion cannot be withdrawn because the company disputes a later enforcement action.

The operating covenant also establishes the public information regime. Physical telemetry is released at a level that permits accountability without exposing details whose disclosure would create a credible security risk. Redactions require stated reasons and independent review. Socioeconomic reports incorporate worker and community evidence rather than relying solely on company-provided statistics.

The covenant is reviewed at fixed intervals and automatically reopened by material changes in load, ownership or control, cooling design, water source, dependence on backup generation, or functional risk class. Its assumptions do not acquire permanent authority merely because they survived the first permit.

### Yellow, Red, and Failure Conditions

In a yellow condition, a protected reserve is declining but immediate safety remains intact. Expansion pauses. Reporting increases. The relevant authority can activate conservation, demand response, or corrective investment.

In a red condition, the system approaches a previously defined boundary. Curtailment, withdrawal limits, emergency pricing protections, or other domain-specific interventions begin. The purpose is not punishment. It is to prevent private output from consuming the reserve needed for public continuity.

In a failure condition, pre-funded recovery mechanisms activate. Responsibility does not depend on proving malicious intent. Workers receive defined transition support. Public infrastructure funds are released. Closure and remediation duties survive bankruptcy to the greatest extent the law can secure. The oversight body conducts a public incident review and revises the operating rules before restart or replacement.

### Expansion Is a New Decision

Large facilities often grow by increments that appear modest when considered separately. The Buffer Commons rejects incremental invisibility. A material expansion triggers cumulative review of the whole facility. Anti-fragmentation rules aggregate adjacent campuses, entities under common control, shared interconnections, staged queue requests, and cumulative regional demand when formal separation would evade review. Existing operations do not create an automatic entitlement to consume the remaining buffer.

This is the point at which technological sovereignty becomes a maintained capability rather than a ceremonial approval. The public does not surrender its future authority at the groundbreaking.

## VII. POLITICAL GEOLOGY AND THE LIMITS OF LOCALISM

The Opal Architecture uses the term **Political Geology** for the durable physical seams through which apparently placeless systems can be governed. Advanced compute depends upon concentrated semiconductor manufacturing, high-voltage electricity, cooling equipment, network connections, financing, specialized labor, and large facilities. These dependencies create points of leverage that software rhetoric can obscure.

But a chokepoint is not automatically a legitimate governor.

Hardware restrictions, export controls, grid tariffs, and manufacturing standards require national or international authority. Land-use decisions and community-benefit conditions may belong to local or

Tribal governments. Transmission reliability belongs to regional institutions. Workplace refusal requires labor law and worker organization. A local community board cannot prevent every offshore deployment, and a national security agency should not decide the distribution of neighborhood burdens.

Claims that physical seams can eliminate jurisdictional arbitrage should also be resisted. Algorithmic efficiency changes the amount of hardware required, and lower energy, water, or hardware use per unit of computation can reduce the cost of additional deployment. Efficiency is not permission. A material efficiency gain, workload change, or utilization increase creates no automatic entitlement to expand total compute volume; it must reopen the covenant and re-demonstrate every protected buffer in absolute, not merely per-unit, terms.[12]

Compute can be distributed. Equipment can be smuggled or repurposed. States may subsidize noncompliance. Some hardware-governance mechanisms remain technically immature or vulnerable to adversarial circumvention.[13]

Physical leverage can reduce arbitrage; it cannot abolish politics.

The appropriate response is nested enforcement. Local institutions govern the burdens that land locally. Regional bodies protect systems whose failure crosses municipal borders. National authorities set non-waivable rights and govern genuinely national chokepoints. International coordination addresses cross-border evasion and prevents wealthy states from defining sovereignty as the right to export extraction.

The objective is not a frictionless global administration. Friction can be protective. The objective is to place each decision at the smallest level capable of governing its consequences, while preserving appeal and coordination where the consequences travel farther.

## VIII. THE HARD OBJECTIONS

Any proposal for democratic technological governance should be tested against the possibility that its own machinery will reproduce the domination it opposes.

### Objection 1: The Buffer Commons Is Another Technocracy

It introduces thresholds, telemetry, audits, trigger conditions, and specialized institutions. The people who define “capacity” could become a new priesthood.

The danger is real. The answer is not to abandon measurement but to bound its authority. Engineering claims require reproducible evidence and independent review. Normative decisions require public reasons, rights, and accountable judgment. Models expose consequences; they do not decide whose life

matters. Communities can challenge baselines and demand alternative analyses. Uncertainty must be displayed rather than laundered into a confident score.

The formula $\mathrm{D} \leq \mathrm{R}$ governs the governor too. Administrative demand must not exceed democratic and epistemic recovery capacity.

## Objection 2: Local Democracy Can Become Exclusion

Communities with wealth and lawyers will protect their buffers while poor communities accept every burden.

This is why local veto alone is inadequate. Regional allocation, anti-discrimination law, minimum protections, public technical assistance, and fiscal equalization are necessary. No locality should be forced to auction its health because ordinary public finance has failed. Equalization must never be conditioned on accepting a project, and refusal must never create a debt to the region. The ability of one community to refuse must not depend on another community's inability to do so.

## Objection 3: Compliance Will Entrench Incumbents

Large firms can finance bonds, lawyers, and audits more easily than small firms and open projects.

This is also true. Obligations must scale along separate physical and functional axes. Public-interest projects need shared evaluation infrastructure, standardized reporting, public compute, legal support, and proportional fees. Regulations should focus on demonstrated exposure rather than treating every act of development as frontier-scale risk.

But "small" and "open" cannot become exemptions from consequence. A low-compute system controlling a critical process may warrant stringent application-level safeguards.

## Objection 4: Companies Will Move

Some will. The threat of exit is part of the present asymmetry. Physical seams, common technical standards, regional coordination, and access to major markets can reduce flight, but no framework can guarantee universal compliance.

The question is not whether every investment can be retained. It is whether retaining a particular investment requires the public to subsidize its risks, surrender essential reserves, or accept terms it would reject if it possessed genuine alternatives.

## Objection 5: UBI Is Too Large and Politically Remote

A national UBI cannot be made a prerequisite for every data-center permit.

Correct. The Buffer Commons distinguishes the general condition of material independence from its complete macroeconomic realization. Project-level refusal rights and unconditional dividends can improve bargaining power now. They do not replace the broader argument for an income sufficient to refuse domination throughout society.

## Objection 6: Compensation Can Purchase Consent

A developer may simply offer enough money to secure approval for a harmful project.

Some impacts are negotiable; others are not. Compensation can distribute benefits and address burdens. It cannot authorize violations of fundamental rights or consume reserves below a protected minimum. The Shielded Core is not for sale.

## Objection 7: This Neglects Catastrophic AI Risk

Data-center water, labor, and ratepayer issues may appear parochial beside the possibility of biological misuse, cyber catastrophe, autonomous conflict, or loss of human control.

The Buffer Commons does not claim that every AI danger reduces to infrastructure. Functional risks require model evaluation, security, access control, incident reporting, and international coordination. The argument is that catastrophic-risk governance also depends on legitimate institutions, protected recovery capacity, and people able to report danger without sacrificing their livelihoods.

Present justice and future safety are not competing budgets of concern. Systems that hide current externalities are unlikely to become honest when the externality is catastrophic. Institutions trained to preserve headroom, disclose uncertainty, fund recovery, distribute authority, and protect refusal are part of the capacity required to confront dangers at every time horizon.

## Objection 8: Buffers Waste Capacity

Unused capacity can look inefficient. A reserve margin produces nothing in ordinary conditions. An escrowed dollar is not invested in expansion. A redundant system appears wasteful until the primary system fails.

This objection reveals the difference between output and persistence. A civilization that consumes every reserve can report impressive utilization immediately before collapse. The buffer is not unused. It is performing the function of keeping failure from becoming irreversible.

### Objection 9: Security Secrecy Will Swallow Accountability

Some infrastructure details, customer identities, and model-risk information cannot safely be made public. A developer or national-security agency may therefore argue that meaningful oversight is impossible.

Secrecy can protect a legitimate interest, but it cannot erase a public burden. Any restriction must be scoped, explained, time-limited where possible, independently reviewable, and subject to appeal. Aggregate electricity, water, emissions, fiscal exposure, incident, and compliance information remains public. Sensitive details may be examined by independent reviewers with appropriate access rather than withheld from every institution outside the operator. No classified or proprietary designation creates an exception to the rights floor, the Shielded Core, or funded repair. If a project cannot support enough independent scrutiny to establish those conditions, it cannot claim informed public consent.

## IX. SOVEREIGNTY AS A MAINTAINED CAPABILITY

Technological sovereignty is often imagined as possession. A country has its own chips. A government has its own cloud. A community has open-source software. A company owns the model. Once the asset is obtained, sovereignty appears complete.

But a population can possess the machine and remain unable to refuse its terms. It can open the code while leaving maintenance unpaid. It can localize the data center while exporting extraction. It can democratize a vote while allowing the majority to consume the minority's safety. It can regulate deployment while leaving no money for repair.

Sovereignty is therefore better understood as a maintained capability.

It is the continuing ability of people to understand a system sufficiently to challenge it; to participate in the rules that govern the resources on which they depend; to refuse work, surveillance, displacement, or danger without losing the means to live; to revise the categories through which ignored harms become visible; to preserve physical and institutional headroom; and to repair damage without begging the failed operator for help.

The Buffer Commons does not abolish markets, states, expertise, private invention, or large infrastructure. It denies any one of them the right to convert public survival into invisible fuel. It places a Genesis Constraint before expansion, Net Buffer Telemetry during operation, a Shielded Core beneath ordinary optimization, and funded repair after failure. It converts the power to say no from a moral wish into an institutional design requirement.

The 100-megawatt facility may still be built. It may provide valuable services, employment, scientific capacity, and public benefit. But it earns admission by preserving the conditions under which the people around it remain free and the larger system remains repairable.

No expansion without headroom.

No consent without the power to refuse.

No innovation without funded repair.

That is not opposition to technological development.

It is the architecture that allows development to belong to the people who must live with what it becomes.

## ENDNOTES

1. Arman Shehabi et al., *2024 United States Data Center Energy Usage Report*, Lawrence Berkeley National Laboratory, December 2024; and US Department of Energy, "DOE Releases New Report Evaluating Increase in Electricity Demand from Data Centers," December 20, 2024. The report estimates 176 TWh of US data-center electricity use in 2023 (4.4 percent of total US electricity) and projects roughly 325–580 TWh in 2028 (6.7–12 percent). LBNL report record; DOE release.
2. Federal Energy Regulatory Commission, "FERC Launches Aggressive Targeted Action to Speed Large Load Integration," June 18, 2026; David Rosner, "Commissioner Rosner's Remarks on the Large Load Show Cause Orders," June 18, 2026. The Commission issued show-cause orders directing six regional grid operators to justify or reform their tariffs; the orders are not a single completed national tariff. Rosner describes Cost Recovery Agreements intended to protect customers from project-specific infrastructure costs, including when a planned large load does not appear. FERC release; Rosner remarks.
3. Elinor Ostrom, "Design Principles in Long-Enduring Irrigation Institutions," *Water Resources Research* 29, no. 7 (1993): 1907–1912, DOI record; Elinor Ostrom, *Governing the Commons: The Evolution of Institutions for Collective Action* (Cambridge University Press, 1990).
4. Eduardo C. Garrido-Merchán, "Commons-Governed Artificial Intelligence: A Taxonomy of Collective Governance," arXiv:2606.15466v1, June 13, 2026, arXiv record. Because this was a recent preprint at the time of writing, it is cited as evidence of an emerging research direction rather than as settled peer-reviewed consensus.
5. European Commission, "Digital Commons EDIC Launches to Advance Europe's Technological Sovereignty," December 11, 2025, European Commission.

6. bell hooks, *Feminist Theory: From Margin to Center* (South End Press, 1984); bell hooks, *Feminism Is for Everybody: Passionate Politics* (South End Press, 2000). The present essay draws on hooks' analysis of domination and the importance of perspectives displaced from institutional centers; it does not claim that hooks wrote about contemporary AI infrastructure.
7. Karl Widerquist, *Independence, Propertylessness, and Basic Income: A Theory of Freedom as the Power to Say No* (Palgrave Macmillan, 2013); Karl Widerquist, "Property and the Power to Say No," DPhil thesis, University of Oxford, 2006, Oxford Research Archive.
8. Yu Tao and Peng Gao, "Global Data Center Expansion and Human Health: A Call for Empirical Research," *Eco-Environment & Health* 4, no. 3 (2025): 100157, DOI record; World Health Organization, "Guidance on Environmental Noise," updated July 3, 2024, WHO guidance. Tao and Gao identify plausible data-center health pathways while emphasizing the need for empirical host-community research. WHO's guidance concerns environmental noise generally, not data centers specifically. These sources support treating directly attributable exposure as a monitored public-health domain; they do not establish that every facility produces harmful exposure.
9. US Environmental Protection Agency, "Financial Assurance Requirements for Hazardous Waste Treatment, Storage and Disposal Facilities," accessed August 10, 2026. EPA describes mechanisms including surety bonds, standby trusts, and letters of credit used to secure closure and post-closure obligations. These rules do not govern data centers; they are cited as an institutional precedent for pre-funded recovery obligations, not as proof that every mechanism is equally protected against insolvency. US EPA.
10. Amelia Michael, *Does the UAE Have an Advantage in Building Data Centers? Comparing the Total Cost of Building and Operating a 100-Megawatt Data Center in the US and the UAE*, GovAI technical report, December 22, 2025. Michael treats the estimates as provisional and confines the comparison to specified total-cost-of-ownership components; the present essay uses the same hypothetical scale for a different institutional inquiry. GovAI report.
11. Regulation (EU) 2024/1689 of the European Parliament and of the Council of June 13, 2024, laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), EUR-Lex. The comparison concerns the general use of differentiated obligations based on risk, not an assertion that the Act implements the Buffer Commons proposed here.
12. Jianxian Wu, "Digital Jevons Paradox in Urban Data Center Energy Systems," *Nature Cities* 2 (2025): 677, DOI record. Wu describes algorithmic efficiency as potentially enlarging rather than reducing AI's total energy footprint. The present essay treats rebound as a governance risk requiring reassessment, not as a fixed ratio or inevitable outcome.
13. Samar Ansari, "Hardware-Level Governance of AI Compute: A Feasibility Taxonomy for Regulatory Compliance and Treaty Verification," arXiv:2604.04712v1, April 6, 2026, arXiv record. The study evaluates multiple hardware-level governance proposals and concludes that several mechanisms most useful for treaty verification remain technically immature or speculative. It is cited as a recent engineering-oriented preprint, not settled consensus or an independent technology-readiness review.

## AI ASSISTANCE DISCLOSURE

Artificial-intelligence tools assisted with research discovery, adversarial review, structural development, and editorial refinement. The framework, synthesis, selection of claims, and responsibility for the published argument remain with Sum Bunny.

## CANON NOTE

This essay develops concepts introduced in Sum Bunny's *The Opal Architecture* (Ark Hive Press, 2026; Sum Bunny Canon no. 207), especially Buffer Mining, Ledger Myopia, the Genesis Constraint, Net Buffer Telemetry, the Shielded Core, and the governing relation $D \leq R$. It converts those general systems concepts into a proposed institutional model for artificial-intelligence infrastructure. It also carries forward the civic-containment and failure-time problem developed in *Smart Machines, Dumb Infrastructure* (2026), the Time-to-Danger account developed in *Failure and Flesh* (2026), the structural account of category blindness developed in *Blind Spot Light* (2025), and the critique of averaging localized harm developed in *The Breath We Buy* (2025).

# APPENDIX: TRANSMISSION

## (NON-ANALYTICAL LAYER)

---

First edition published on the Internet Archive, 2026.

Part of the Sum Bunny Canon (Ark Hive Press).

This work was developed with AI-assisted analysis tools. All arguments, structures, and final judgments are the author’s.

This edition preserves the essay’s analytical text, citations, and verified endnotes as of August 10, 2026.

**NO EXPANSION WITHOUT HEADROOM.**

**NO CONSENT WITHOUT THE POWER TO REFUSE.**

**NO INNOVATION WITHOUT FUNDED REPAIR.**

Hey Josiane,

**Sum Bunny Loves You!!!**

ARK HIVE PRESS · OPEN THROTTLE · CC BY 4.0